GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición º2223

En alianza con

TD SYNNEX FORTINET

# BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

## VISTA RÁPIDA

| | CRÍTICO | URGENTE | IMPORTANTE |
|---|---|---|---|
| VULNERABILIDADES | 4 | | |
| MALWARE | | 3 | 2 |
| BRECHAS DE SEGURIDAD | | 1 | |
| NOTICIAS DE CIBERSEGURIDAD | 1 | 1 | 2 |
| SECTOR FINANCIERO | 1 | | |

## VULNERABILIDADES

### Zyxel parchea vulnerabilidad en dispositivos NAS

Zyxel ha parcheado una vulnerabilidad de inyección de comando autenticado de alta gravedad (CVE-2023-27988) en algunos de sus dispositivos de almacenamiento conectado a la red (NAS) destinados a usuarios domésticos.

**Prioridad: 1 Crítico.**

**Ampliar información:**

- https://www.helpnetsecurity.com/2023/05/31/cve-2023-27988/

---

## Vulnerabilidad de manipulación de datos en plugin de WordPress

La empresa de software que está detrás de la plataforma de blogs WordPress, está actualizando automáticamente más de cinco millones de instalaciones en su plugin Jetpack después de que se descubriera una vulnerabilidad crítica en él.

**Prioridad: 1 Crítico.**

**Ampliar información:**

- https://www.cert.gov.py/noticias/vulnerabilidad-de-manipulacion-de-datos-en-plugin-de-wordpress/
- https://thehackernews.com/2023/06/urgent-wordpress-update-fixes-critical.html

---

## Modelos de placas base Gigabyte vulnerables

Gigabyte, uno de los mayores fabricantes de hardware del mundo, incluye en el firmware de "cientos de modelos" de sus placas base, una vulnerabilidad que permite instalar puerta trasera o backdoor ya que durante el proceso de inicio del sistema es capaz de descargar y ejecutar payloads de forma insegura, según ha descubierto el equipo de investigadores de firma de seguridad Eclypsium.

**Prioridad: 1 Crítico.**

**Ampliar información:**

- https://www.wired.com/story/gigabyte-motherboard-firmware-backdoor/

- https://eclypsium.com/blog/supply-chain-risk-from-gigabyte-app-center-backdoor/
- https://www.gigabyte.com/Press/News/2091

---

## Nueva vulnerabilidad de hardware en procesadores Intel

Un grupo de investigadores de la Universidad de Maryland en los EE. UU. y la Universidad de Tsinghua en China, publicaron un artículo científico que documenta un nuevo método de ataque de canal lateral que explota una vulnerabilidad de hardware previamente desconocida en los procesadores Intel.

**Prioridad: 1 Crítico.**

**Ampliar información:**

- https://arxiv.org/pdf/2304.10877.pdf
- https://latam.kaspersky.com/blog/transient-cpu-eflags/26367/

---

## Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.

- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

## MALWARE

### Lazarus apunta a servidores IIS para el acceso inicial y mediante DLL Hijacking

Delincuentes informáticos respaldados por el estado de Corea del Norte, conocidos como Lazarus Group, ahora tienen como objetivo los servidores web vulnerables de Windows Internet Information Services (IIS), para obtener acceso inicial a redes corporativas.

**Prioridad: 2 Urgente.**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/lazarus-hackers-target-windows-iis-web-servers-for-initial-access/
- https://blog.segu-info.com.ar/2023/05/lazarus-apunta-servidores-iis-para-el.html

---

### Un nuevo malware vinculado a Rusia, supone una “amenaza inmediata” para las redes energéticas

Un nuevo malware vinculado a Rusia y diseñado para derribar las redes eléctricas ha sido identificado por los investigadores de amenazas de Mandiant, que han instado a las empresas energéticas a tomar medidas para mitigar esta "amenaza inmediata."
El malware especializado en tecnología operativa (OT), apodado COSMICENERGY, tiene similitudes malware utilizado en ataques anteriores dirigidos a redes eléctricas, incluido el incidente 'Industroyer' que dejó sin electricidad a Kiev, Ucrania, en 2016.

**Prioridad: 2 Urgente.**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/new-russian-linked-cosmicenergy-malware-targets-industrial-systems/
- https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html

---

## Qilin / Agenda ransomware activo en América Latina

En un estudio de investigación, el equipo de inteligencia de amenazas de Group-IB dijo que se infiltró y analizó el funcionamiento interno de ransomware Qilin, revelando información sobre sus objetivos en sectores críticos y las técnicas sofisticadas que emplearon.

Qilin, también conocido como ransomware Agenda, se ha convertido en una amenaza importante desde su descubrimiento en agosto de 2022, según el estudio. Se ha observado que el grupo desarrolla nuevo malware utilizando el lenguaje de programación Rust y lo ha usado para atacar varias empresas.

**Prioridad: 2 Urgente.**

**Ampliar información:**

- https://www.infosecurity-magazine.com/news/qilin-ransomware-targets-critical/
- https://www.group-ib.com/blog/qilin-ransomware/

---

## Pegasus tiene un sustituto como software espía en Estados Unidos: Graphite

El gobierno de EEUU prohibió Pegasus de NSO, pero compra el spyware rival Paragon Graphite, con la creciente controversia en torno al uso de software espía por parte de los gobiernos, es evidente que el debate sobre la seguridad nacional y la privacidad individual está lejos de terminar.

**Prioridad: 3 Importante.**

**Ampliar información:**

- https://www.digitalinformationworld.com/2023/05/new-report-says-american-government.html
- https://9to5mac.com/2023/05/30/paragon-graphite/

---

## Incidente de seguridad informática en ABB basado en ransomware

Recientemente, ABB, una reconocida empresa, ha sido víctima de un incidente de seguridad informática que ha afectado a algunos de sus sistemas. Sin embargo, según el comunicado emitido por la empresa, se han tomado medidas inmediatas para contener y evaluar el incidente.

Según la información proporcionada por ABB, el acceso no autorizado a ciertos sistemas fue perpetrado por un tercero que desplegó un tipo de ransomware que no se propagaba automáticamente.

**Prioridad: 3 Importante.**

**Ampliar información:**

- https://cybersecuritynews.es/incidente-de-seguridad-informatica-en-abb-basado-en-ransomware/
- https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/

---

## Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.
- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.

- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

## BRECHAS DE SEGURIDAD

### Banco español confirma ataque de ransomware

Un importante prestamista en España dijo que está lidiando con un ataque de ransomware que afecta a varias oficinas. Globalcaja, con sede en la ciudad española de Albacete, tiene más de 300 oficinas en toda España y atiende a casi medio millón de personas con una variedad de servicios bancarios. Administra más de $ 4.6 mil millones en préstamos de consumo y tiene 1.000 empleados.

**Prioridad: 2 Urgente.**

**Ampliar información:**

- https://therecord.media/spain-globalcaja-bank-confirms-ransomware-attack

## NOTICIAS DE CIBERSEGURIDAD

### Ciberataque obliga a un hospital en Idaho Falls a enviar ambulancias a otro lugar

Debido al daño causado a los sistemas informáticos del hospital por un hackeo, las ambulancias que atienden a una amplia población en Idaho están siendo desviadas para ser tratadas en otras clínicas. El Hospital Comunitario de Idaho Falls no respondió a las consultas sobre la duración del tiempo. Anticipan que sería necesario redirigir a los pacientes de emergencia; sin embargo, el hospital sí dijo en un comunicado que hizo en la página de Facebook del martes que ha estado luchando contra el ataque cibernético desde el lunes por la mañana.

**Prioridad: 1 Crítico.**

**Ampliar información:**

- https://noticiasseguridad.com/hacking-incidentes/ciberataque-obliga-a-un-hospital-grande-a-enviar-ambulancias-a-otro-lugar/

---

## ChatGPT eleva el nivel de sofisticación del ciber fraude

La llegada de ChatGPT se ha convertido rápidamente en un tema muy discutido, especialmente por los numerosos usos que pueden darse a la inteligencia artificial (IA). Los criminales no han tardado en encontrar nuevas y maliciosas maneras con las que delinquir apoyándose en las infinitas posibilidades que ofrece la herramienta. De hecho, el último informe de Europol revela que con ChatGPT los ciberdelincuentes pueden crear estafas más sofisticadas y a un ritmo más rápido, lo que dificulta todavía más su detección.

**Prioridad: 3 Importante.**

**Ampliar información:**

- https://cybersecuritynews.es/chatgpt-eleva-el-nivel-de-sofisticaccion-del-ciberfraude/

## Abogados usaron ChatGPT para demandar a Avianca y la IA se inventó casos y testigos

Roberto Mata, un hombre que viajaba de El Salvador a Nueva York, denunció a Avianca porque, al parecer, un carrito de servicio de metal golpeó su rodilla durante el vuelo. La aerolínea colombiana pidió que se desestimara el caso ante un juez federal de Manhattan. Sin embargo, los abogados de Mata contraatacaron con un contundente escrito que refería a más de media docena de decisiones judiciales que favorecían la demanda. ¿El problema? Casi todos estos casos eran falsos.

**Prioridad: 3 Importante.**

**Ampliar información:**

- https://hipertextual.com/2023/05/abogados-usaron-chatgpt-demanda-aerolinea-avianca

## Nueva técnica de phishing permite hackear a alguien usando dominios .zip y .mov

Cuando una víctima visita un sitio web que termina en .ZIP, se puede usar un método de phishing desarrollado recientemente conocido como “archivador de archivos en el navegador” para “emular” el software de archivo de archivos en el navegador web del objetivo.
Según la información publicada por un investigador de seguridad llamado mr.d0x la semana pasada, “con este ataque de phishing, simula un software de archivado de archivos (por ejemplo, WinRAR) en el navegador y usa un dominio .zip para que parezca más legítimo”.

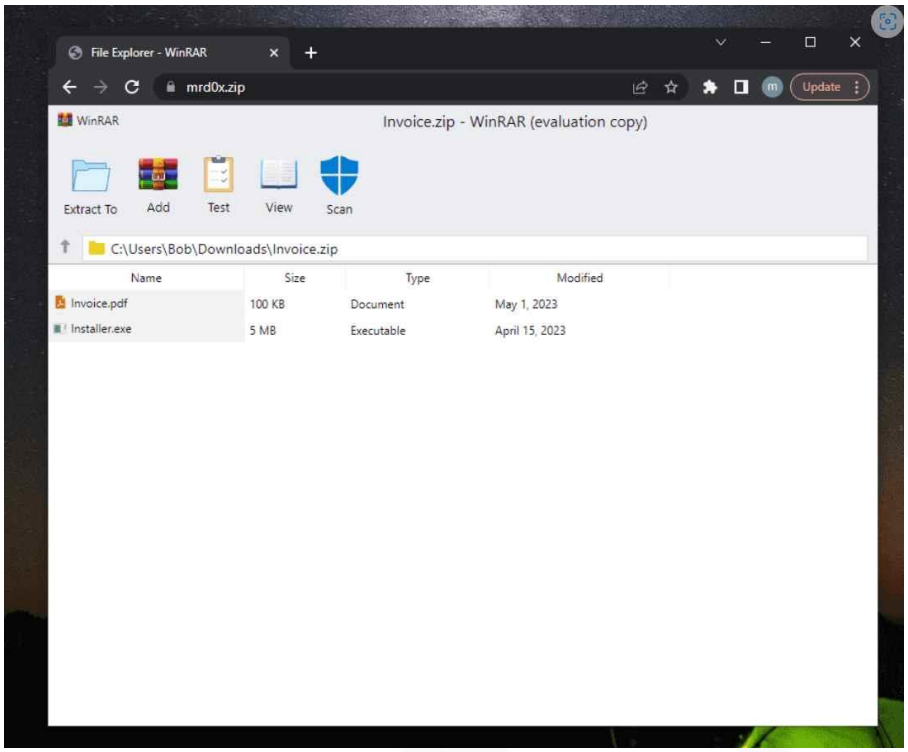


Imagen de prueba de concepto de la técnica.

**Prioridad: 2 Urgente.**

**Ampliar información:**

- https://noticiasseguridad.com/seguridad-informatica/nueva-tecnica-de-phishing-permite-hackear-a-alguien-usando-dominios-zip-y-mov/